



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/654,436	09/01/2000	Akira Takura	13700-0250	5758

23370 7590 05/24/2004

JOHN S. PRATT, ESQ
KILPATRICK STOCKTON, LLP
1100 PEACHTREE STREET
SUITE 2800
ATLANTA, GA 30309

EXAMINER

KIM, JUNG W

ART UNIT	PAPER NUMBER
----------	--------------

2132

DATE MAILED: 05/24/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

22

Office Action Summary

Application No.

09/654,436

Applicant(s)

TAKURA ET AL.

Examiner

Jung W Kim

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-37 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-37 is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 01 September 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. ____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 3.4.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: ____.

DETAILED ACTION

1. Claims 1-37 have been examined.

Specification

2. The disclosure is objected to because of the following informalities: on page 1, line 22, an indefinite article is missing; on page 5, lines 8-16, the sentence is not grammatical. Appropriate correction is required.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

5. Claims 1-2, 7, 11-12, 20-21, 28-29, and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Haber et al. U.S. Patent No. 5,136,647 (hereinafter Haber) in view of Rohatgi et al. U.S. Patent No. 5,625,693 (hereinafter Rohatgi). As per claim 1, Haber discloses a time stamping system, comprising a client device and a server device (see Haber, Figures 1 and 2);

- a. the client device including:
 - i. a digest generation unit for generating a digest for a digital document (see Haber, col. 5, line 57-col. 6, line 5),
 - ii. a transmission unit for transmitting a time stamping request containing the digest generated by the digest generation unit to the server device (see Haber, col. 6, lines 5-15), and
 - iii. a reception unit for receiving a time stamp token for the digital document from the server device (see Haber, col. 6, line 67-col. 7, line 3); and
- b. wherein the server device generates the time stamp token containing a time stamped digital document obtained by combining the digest and a time information acquired in response to the time stamping request, and a digital signature for the time stamped digital document (see Haber, col. 6, lines 16-65).

Haber is silent on means for generating a plurality of digests for a plurality of digital documents, wherein the digests are combined and a unified digest is generated from the plurality of digests. However, means to create a unified digest from a plurality of

digests are found in several inventions to establish a verification system by fingerprinting at least one document and fingerprinting a registry holding the at least one document fingerprint. For example, Rohatgi discloses such a means to create a unified digest from a plurality of digital documents (see Rohatgi, col. 8, lines 37-60, especially lines 42-45 and 54-58). It would be obvious to one of ordinary skill in the art at the time the invention was made to apply the teaching of Rohatgi to the invention disclosed by Haber. Motivation for such a combination would ensure a more secure means of fingerprinting by creating multiple levels of hashes. The aforementioned covers claim 1.

6. As per claim 2, Haber covers a time stamping system as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, the client device further includes a digital document specifying unit for specifying the plurality of digital documents from digital documents on a personal computer or a network, in units of files or folders (see Rohatgi, col. 4, lines 10-29, especially lines 11-13; col. 9, lines 42-61).

7. As per claim 7, Haber covers a time stamping system as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, the server device includes:

- a. a digital signature generation unit for obtaining the time stamped digital document by combining the unified digest and the time information, and generating the digital signature for the time stamped digital document (see Haber, col. 6, lines 23-50); and

- b. a time stamp token generation unit for generating the time stamp token from the time stamped digital document and the digital signature generated by the digital signature generation unit (see Haber, col. 7, lines 1-14).

The aforementioned covers claim 7.

8. As per claims 11-12, 20-21, 28-29, and 36, they are claims corresponding to claims 1-2 and 7 and they do not teach or define above the information claimed in claims 1-2 and 7. Therefore, claims 11-12, 20-21, 28-29, and 36 are rejected as being unpatentable over Haber in view of Rohatgi for the same reasons set forth in the rejections of claims 1-2 and 7.

9. Claims 4, 14, 23, and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Haber in view of Rohatgi, and further in view of Walker et al. U.S. Patent No. 5,768,382 (hereinafter Walker). As per claim 4, Haber covers a time stamping system as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). Haber is silent on a time specifying unit at the client device for specifying regular digest generation times for the plurality of documents. However, Walker teaches periodically generating hashes of previously hashed documents to check if the documents have changed over the course of a period (see Walker, col. 18, line 35-col. 19, line 19). It would be obvious to one of ordinary skill in the art at the time the invention was made to apply the teaching of Walker to the invention covered by Haber. Motivation for such an

implementation would enable periodic checks if the original documents were surreptitiously modified.

10. As per claims 14, 23, and 31, they are claims corresponding to claim 4 and they do not teach or define above the information claimed in claim 4. Therefore, claims 14, 23, and 31 are rejected as being unpatentable over Haber in view of Rohatgi and Walker for the same reasons set forth in the rejection of claim 4.

11. Claims 3, 5, 13, 15, 22, 24, 30, and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Haber in view of Rohatgi, and further in view of Epstein. As per claim 5, Haber covers a time stamping system as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, Haber teaches validation steps to verify the authenticity of a digital signature received by server (see Haber, col. 7, lines 15-24), but does not teach a validation means at the client device. Epstein teaches a validation means at a client device when a client desires to revise a document and verifies that the document to be revised is the original document (see Epstein, Figure 1C). It would be obvious to one of ordinary skill in the art at the time the invention was made to apply the teaching of Epstein to the invention covered by Haber. Motivation for such a combination enables the client to verify the authenticity and integrity of a document.

12. As per claim 3, Haber covers a time stamping system as outlined above in the claim 2 and 5 rejections under 35 U.S.C. 103(a). In addition, the digital document

specifying unit specifies the plurality of digital documents such that a previously obtained time stamp token is included in the plurality of digital documents (see Rohatgi, col. 4, lines 10-29, especially lines 11-13; col. 9, lines 42-61 as modified by Epstein, Figure 1C, Reference No. 123).

13. As per claims 13, 15, 22, 24, 30, and 32, they are claims corresponding to claims 3 and 5 and they do not teach or define above the information claimed in claims 3 and 5. Therefore, claims 13, 15, 22, 24, 30, and 32 are rejected as being unpatentable over Haber in view of Rohatgi and Epstein for the same reasons set forth in the rejections of claims 3 and 5.

14. Claims 6, 16, 25, and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Haber in view of Rohatgi, and further in view of Stallings Cryptography and Network Security 2nd Edition (hereinafter Stallings). As per claim 6, Haber covers a time stamping system as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). Haber is silent on a verification unit to verify that the time indicated by the time stamped digital document is a valid time. Stallings teaches a simple routine to verify that received timestamps are within a valid transmission time between two nodes (see Stallings, page 306, 2nd paragraph). It would be obvious to one of ordinary skill in the art at the time the invention was made to apply the teaching of Stallings to the invention taught by Haber. Motivation for such a combination enables the invention to verify the time of a timestamp as valid.

15. As per claims 16, 25, and 33, they are claims corresponding to claim 6 and they do not teach or define above the information claimed in claim 6. Therefore, claims 16, 25, and 33 are rejected as being unpatentable over Haber in view of Rohatgi and Stallings for the same reasons set forth in the rejection of claim 6.

16. Claims 8-10, 17-19, 26-27, 34-35, and 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Haber in view of Rohatgi, and further in view of Schneier, Applied Cryptography 2nd Edition (hereinafter Schneier). As per claims 8 and 10, Haber covers a time stamping system as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). Although Haber is silent on the matter of a plurality of digital signature units formed from a plurality of time acquisition units to form a unified digital signature and corresponding token, one of the common issues with timestamping is ensuring that the timestamp created by a producer is legitimate (see Schneier, page 75, 3rd bullet; page 76, 5th paragraph). One principle means of ensuring the legitimacy of a timestamp is to receive partial timestamps from a plurality of producers to create a legitimate timestamp. As taught by Schneier, this idea is called secret splitting, and requires a plurality of producers to provide legitimate partial secrets to create a legitimate full secret (see Schneier, pages 70-71, section 3.6 'Secret Splitting'). This means prevents forgery of a secret, in the case of a timestamping system, a specific time associated with a document. Further, in a different section, Schneier teaches a general improved arbitrated solution for generating timestamps wherein a timestamp generator receives a

hash from a sender, appends a timestamp, digitally signs the result then sends everything back to the sender (see Schneier, page 76, 'Improved Arbitrated Solution'). Hence, in a timestamping splitting system, each partial timestamp producer generates a timestamp, along with the partial secret, signs the result then submits the result to a central station to form the secret (and hence a unified digital signature). It would be obvious to one of ordinary skill in the art at the time the invention was made to apply the teaching of Schneier to the invention covered by Haber. Motivation for such an implementation reduces the risk of a timestamp forgery. The aforementioned cover claims 8 and 10.

17. As per claim 9, Haber covers a timestamping system as outlined in the claim 8 rejection under 35 U.S.C. 103(a). In addition, the limitations defined by a claim that ensure the correct operation of an invention are inherent features of an invention. Hence, claim 9 is covered by the invention taught by Haber as modified by Rohatgi and Schneier.

18. As per claims 17-19, 26-27, 34-35, and 37, they are claims corresponding to claims 8-10 and they do not teach or define above the information claimed in claims 8-10. Therefore, claims 17-19, 26-27, 34-35, and 37 are rejected as being unpatentable over Haber in view of Rohatgi and Schneier for the same reasons set forth in the rejections of claims 8-10.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.


Ishii U.S. Patent No. 5,768,389.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is (703) 305-8289. The examiner can normally be reached on M-F 9:00-6:00.

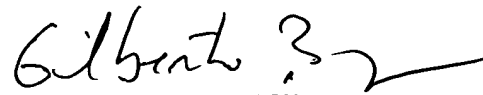
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jk



Jung W Kim
Examiner
Art Unit 2132



GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Application/Control Number: 09/654,436

Art Unit: 2132

Page 11

May 13, 2004